CC

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-173972
(43)Date of publication of application : 13.07.1993

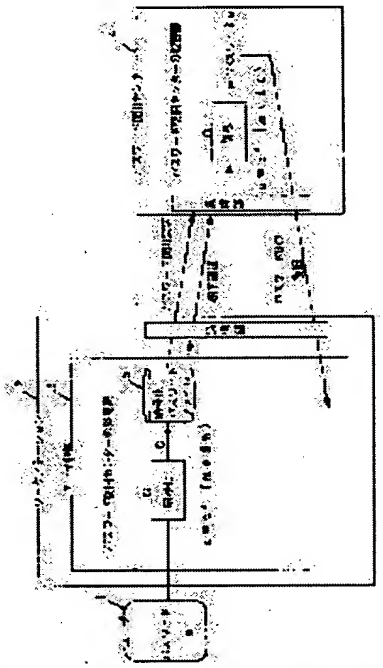
(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 9/06
H04L 9/14

(21)Application number : 03-341012
(22)Date of filing : 24.12.1991

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(54) PASSWORD RESTORING METHOD

(57)Abstract:
PURPOSE: To provide a method for restoring a lost password and a method for confirming an inputted password without impairing safety nor easiness.
CONSTITUTION: A password restoration center 4 which restores the password is provided and a user ciphers his or her password by using the open key of the password restoration center 4 and then stores it. If the password is lost, the user indicates the ciphered and stored password and requests the password restoration center 4 to restore the password. The password restoration center 4 after certifying the user 1 deciphers the ciphered password by using a secret key and informs the user 1 of the result. Then the ciphered password is stored on a portable medium and identification information, etc., the user 1 is ciphered at the same time. The ciphered password is used to confirm whether or not the inputted password is correct.



LEGAL STATUS

[Date of request for examination] 17.03.1997
[Date of sending the examiner's decision of rejection] 21.03.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－173972

(43)公開日　平成5年(1993)7月13日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｅ	8219－5L		
	13/00	３５１　Ｚ	7368－5B		
Ｈ０４Ｌ	9/06				
	9/14				
			7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数６(全　7　頁)

(21)出願番号　特願平3－341012

(22)出願日　平成３年(1991)12月24日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　パスワード復旧方法

(57)【要約】

【目的】　①安全性、簡易性を損なうことなく紛失したパスワードを復旧する方法を提供する。

②入力されたパスワードの確認方法を提供する。

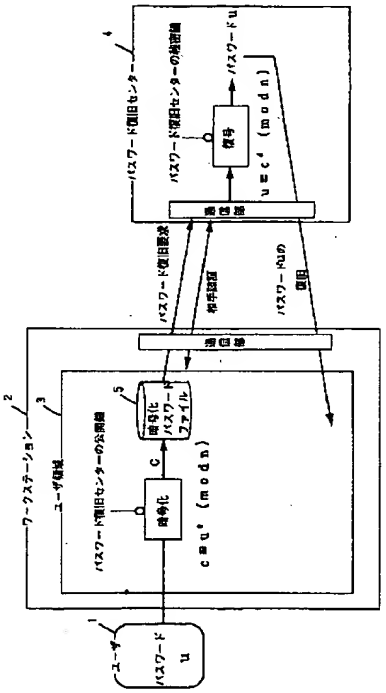
【構成】　①パスワードの復旧を行うパスワード復旧センターを備え、ユーザは自分のパスワードをパスワード復旧センターの公開鍵を用いて暗号化した上で保管する。万一パスワードを紛失したときには、この保管している暗号化したパスワードを提示してパスワード復旧センターにパスワード復旧を要求する。パスワード復旧センターはユーザの認証を行った後、秘密鍵により暗号化パスワードを復号し、その結果をユーザに通知する。

②前記暗号化パスワードを可搬媒体に格納する。

③ユーザの識別情報等も同時に暗号化する。

④暗号化されたパスワードを入力されたパスワードの正否の確認に使用する。

【効果】



1

【特許請求の範囲】

【請求項１】　パスワード復旧センターが自己の秘密鍵を保持し、それに対する公開鍵をユーザに公開するステップと、ユーザが自己のパスワードを前記公開鍵を用いて暗号化し、その結果を暗号化パスワードとして保持するステップと、ユーザがパスワードを紛失した場合には前記暗号化パスワードを前記パスワード復旧センターに提示して前記パスワードの復旧を請求するステップと、パスワード復旧センターが前記提示された暗号化パスワードを前記秘密鍵を用いて復号するステップと、その復号結果をユーザに通知するステップとを有することを特徴とするパスワード復旧方法。

【請求項２】　前記暗号化パスワードを可搬媒体に保持することを特徴とする請求項１記載のパスワード復旧方法。

【請求項３】　前記パスワードに替えてパスワードとユーザ固有の識別情報との結合である結合パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２記載のパスワード復旧方法。

【請求項４】　前記パスワード若しくは結合パスワードに替えて、ユーザがパスワードに秘密処理を行った秘密パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２若しくは３記載のパスワード復旧方法。

【請求項５】　複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが一個のパスワードとして暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２若しくは３若しくは４記載のパスワード復旧方法。

【請求項６】　入力されたパスワードを前記パスワード復旧センターの公開鍵を用いて暗号化するステップと、このステップで得た暗号化パスワードと保持している前記暗号化パスワードとを比較することによって前記の入力値が正しいパスワードか否かを確認するステップとを有することを特徴とするパスワード入力の正否確認方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】パスワードを紛失した場合の復旧方法に関する。

【０００２】

【従来の技術】近年、開放的なワークステーションネットワークが普及する一方、ワークステーションで取り扱う情報の重要性が増してきている。これらのことを背景に、ワークステーション間のデータのやり取り、データベースの蓄積などに暗号化技術が導入されてきている。

【０００３】例えば、他者に見られたくない内容のファイルはユーザの設定した数値情報たるパスワード（鍵）で、暗号化した上で保管しておけばよい。この場合の暗号方式としては、その便利さ故に暗号化と復号に同じ鍵

2

を用いる共通鍵暗号方式が一般的に用いられている。この方式においては、パスワードを知っているユーザ本人だけが、ファイルを暗号化する際に用いたパスワードで暗号化ファイルを復号してもとの内容を得ることが出来るため、その安全性は高い。

【０００４】ところが、この場合に、もしユーザが自分の設定したパスワードを紛失してしまったなら、暗号化して保管しておいたファイルからもとの内容を復旧することができなくなる。又パスワードを個人認証に用いている銀行の預貯金オンラインシステム等においても、そのパスワードを紛失すると、カードを使った引き出し、預け入れ等が不可能になってしまう。そのため、従来はこの大切なパスワードを、紛失しないように例えば紙などに書き付けて携帯するか、ワークステーションのそばにおいておくというようなことがなされていた。

【０００５】

【発明が解決しようとする課題】しかし、このような紛失対策はシステムの安全性を損なうため，本来的には好ましくない。すなわち、安全性の面からパスワードはそれを設定した本人の記憶だけに蓄えられるべきである。といってユーザが自分の設定したパスワードを失念等することにより紛失してしまうのを完全に防止するのは困難である。ところで、ファイルシステムの場合、ファイルの内容が重要であればあるほど、安全性確保の面からパスワードは長くなりがち（桁が大きくなりがち）であり、また近年パスワードを多数使用することが多くなり、これらの面からも失念等しやすい。

【０００６】この場合、オンラインシステムを利用しての銀行への預貯金であるならば、パスワードやマネーカードを紛失しても、別途預貯金通帳と印鑑の提出等による復旧がなされ得る。しかし、再発行の手間は大変である。一方、ＬＡＮ、通信回線等の開放的なワークステーションネットワークを利用するデータベースの蓄積等においては、いかなる手段を使用してももとの情報を復旧することはできない。しかるに、従来、安全かつ簡易に紛失したパスワードを復旧する対策が用意されていなかった。そのためワークステーションを利用してのデータベースの蓄積等においては、その便利さは認識されつつも暗号化システムがあまり普及しない原因となっていた。

【０００７】本発明は、安全かつ簡単なパスワードを復旧する方法を提供することにより上記問題点を解決する目的でなされたものである。

【０００８】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明に係るパスワード復旧方法においては、パスワード復旧センターが自己の秘密鍵を保持し、それに対する公開鍵をユーザに公開するステップと、ユーザが自己のパスワードを前記公開鍵を用いて暗号化し、その結果を暗号化パスワードとして保持するステッ

プと、ユーザがパスワードを紛失した場合には前記暗号化パスワードを前記パスワード復旧センターに提示して前記パスワードの復旧を請求するステップと、パスワード復旧センターが前記提示された暗号化パスワードを前記秘密鍵を用いて復号するステップと、その復号結果をユーザに通知するステップとを有することを特徴としている。

【０００９】請求項２の発明に係るパスワード復旧方法においては、前記暗号化パスワードを可搬媒体に保持することを特徴とする請求項１記載のパスワード復旧方法としている。請求項３の発明に係るパスワード復旧方法においては、前記パスワードに替えてパスワードとユーザ固有の識別情報等の結合である結合パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２記載のパスワード復旧方法としている。

【００１０】請求項４の発明に係るパスワード復旧方法においては、前記パスワード若しくは結合パスワードに替えて、ユーザがパスワードに秘密処理を行った秘密パスワードが暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２若しくは３記載のパスワード復旧方法としている。請求項５の発明に係るパスワード復旧方法においては、複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが一個のパスワードとして暗号化され、暗号化パスワードとされることを特徴とする請求項１若しくは２若しくは３若しくは４記載のパスワード復旧方法としている。

【００１１】請求項６の発明に係るパスワード入力正否確認方法においては、入力されたパスワードを前記パスワード復旧センターの公開鍵を用いて暗号化するステップとこのステップで得た暗号化パスワードと、保持している前記暗号化パスワードを比較することによって前記別の入力値が正しいパスワードか否かを確認するステップとを有することを特徴としている。

【００１２】

【作用】以上の構成により、請求項１の発明においては、ユーザから提示された公開鍵を使用して暗号化されたパスワードに対し、パスワード復旧センターが自己の秘密鍵を使用することにより復号をなし、その結果をユーザに通知することがなされる。

【００１３】請求項２の発明においては、ユーザがパスワードを可搬媒体に保管する。請求項３に係る発明においては、結合パスワードが暗号化され、暗号化パスワードとされる。請求項４に係る発明においては、秘密パスワードが暗号化され、暗号化パスワードとされる。

【００１４】請求項５に係る発明においては、複数の、パスワード若しくは結合パスワード若しくは秘密パスワードが暗号化され、暗号化パスワードとされる。請求項６に係る発明においては、入力されたパスワードを公開鍵を用いて暗号化したパスワードと、あらかじめ保持している暗号化パスワードとの比較がなされることにより、入力されたパスワードの正否確認がなされる。

【００１５】

【実施例】以下、請求項１の発明を実施例に基づき説明する。図１は本発明に係るパスワード復旧方式の一実施例の構成を示すものである。本図において、１はユーザ、２はユーザの用いている開放的なワークステーション、３はワークステーション内のユーザ１の領域、４はパスワード復旧センターである。パスワード復旧センター４はユーザのワークステーション２とは別の機関であり、ユーザのパスワードの復旧を行なう場合のみユーザとの情報交換を行う。以下、本図を用いて本実施例の動作を説明する。

【００１６】まず、パスワード復旧センター４はある公開鍵暗号方式を決定し、この公開鍵暗号方式における秘密の数値情報たる秘密鍵を保持し、この秘密鍵に対する公開の数値情報たる公開鍵をユーザ１に公開する。本実施例では公開鍵暗号方式として、ＲＳＡ暗号方式を用いている。本ＲＳＡ暗号方式は、１９７８年にリベスト、シャミア、アドルマン、の３人によって提案された公開鍵暗号方式で、’アメソド　オブ　オブテイニング　ディジタル　シグネチャズアンド　パブリックキー　クリプトシステムズ”（R. L. Ribvest, A. Shamirand L. Adleman:”A method of obtainingdigital signatures and public key cryptosystems”, Comm. of ACM, pp. １２０－１２６（FEB. １９７８））に詳しく述べられており、我国の文献では池野　信一、小山　謙二　共著、電子通信学会発行「現代暗号理論」の第六章に説明されている。

【００１７】なお、ＲＳＡ暗号の要旨は以下の通りであるＲＳＡ暗号においては、暗号鍵は（ｅ，ｎ）の組であり、復号鍵は（ｄ，ｎ）である。暗号鍵は公開される。そして暗号化と復号アルゴリズムはそれぞれ、平分をＭ、暗号文をＣとすると、

暗号化は　　$C \equiv M^e \pmod n$

復号は　　$M \equiv C^d \pmod n$

で表される。なお、（mod n)は整数Ｃ、Ｍをｎで除したときの剰余を示す。上記式はフェルマーの定理より、ｅ×ｄ≡１（mod m)とすることにより成りつ。ここで、ｍはｎのオイラー（ＥＵＬＥＲ）の関数値であり、ｎ以下かつｎと互いに素な正整数の個数を表す。そしてｎ＝ｐ×ｑ（ｐ，ｑ：素数）としたとき、ｍは（ｐ－１）と（ｑ－１）の最小公倍数となる。

【００１８】そしてこのＲＳＡ暗号の安全性は、

（１）暗号文Ｃと公開鍵ｅよりもとの平文Ｍが求められないこと。数学（整数論）でいう指数計算、通信学でいう離散対数問題の困難性により、ｎを十分大きく取ると、ＣよりＭを求めることは困難となる。

（２）公開鍵ｅよりｄが求められないこと。

【００１９】数学における素因数分解の困難性により、ｎの素因数であるｐ，ｑを十分に大きくとることによりｄを求めることは困難となる。による。以上のもとで、パスワードの暗号化と復号の手順を以下に示す。パスワード復旧センター４は、秘密の素数ｐ，ｑと両者の積ｎとｅ×ｄ≡１ｍｏｄｍを満たすｅ，ｄを求めて、（ｐ，ｑ，ｄ）を秘密情報として保持し、（ｎ，ｅ）をユーザ１に公開する。

【００２０】ユーザ１は、自己の設定した秘密の数値情報たるパスワードｕを上記パスワード復旧センター４の公開鍵を用いて以下の計算により暗号化する。その結果である暗号化パスワードｃは、ワークステーション上のユーザ１の暗号化パスワードファイル５を作成して、これに格納して保管しておく。

$c \equiv u^e \pmod{n}$（ｕ：パスワード、ｃ：暗号化パスワード。）…（数１）

そして、この操作はユーザ１が新規にパスワードｕを登録するとき、あるいはパスワードを更新するときに行われる。なお、ここでの暗号化パスワードファイル５はパスワード復旧センターの公開鍵で暗号化されているため、ワークステーション内の他のユーザに知得されたとしても、安全性が損なわれる危険性はない。すなわち、ｎとｃとｅとからｕをもとめるは、非常に困難である。

【００２１】さて、ユーザが使用している自己のパスワードｕを万一紛失したときには、ユーザ１はこの保管している暗号化パスワードファイル５内の暗号化パスワードｃを、ワークステーション及びパスワード復旧センターの通信部を経由してパスワード復旧センターに通知し、パスワードの復旧を要求する。、パスワード復旧センターはユーザ１の認証、すなわち復旧を要求している者がたしかにユーザ１であることの確認、を行う。そして、自分の秘密鍵を用いて以下の計算を行ない、パスワードｕを復旧し、その結果をユーザ１に送信する。

【００２２】$u \equiv c^d \pmod{n}$ …（数２）

なお、この場合にパスワード復旧センターとユーザ１との通信が公開ネットワークを利用する場合には、第三者の詐称に対する防衛が必要であり、このための認証方法についても種々発明がなされており、本出願人等も別途特願平３－１９９１４８号、特願平４－３３７１２５号にて出願をなしているが、これらは本発明の要旨には直接に関係しないため、その説明は省略する。パスワード復旧センターからの送信内容を受信したユーザ１はこの復旧されたパスワードｕを用いて、新しいパスワードを設定し直し、暗号化パスワードファイル５を更新する。なお、同時に、もとのパスワードを用いて暗号化している暗号化ファイルがある場合は復旧されたパスワードを用いて復号し、その上で新しく設定したパスワードで新しく暗号化し直す操作も行う。

【００２３】次に、この方法の安全性について説明する。まず、ユーザがパスワードを記憶している間は、ユーザの暗号化パスワードファイルは、ワークステーション２内のユーザ１の領域３に格納されている。その領域３はワークステーションに備わるアクセス管理メカニズムによりパスワード復旧センターがユーザとの間の通信手段を使用して知得することができないようになっている。そのため、パスワード復旧センター４は、ユーザ１のパスワードを求めることはできない。また、ユーザ１が、暗号化パスワードを提示してパスワードの復旧を求めてきたときには、パスワード復旧センター４は自身の秘密鍵を用いてこれを復号し、ユーザ１のパスワードを得ることはできる。しかしながら、復旧したパスワードをユーザ１に送信した時点で、ユーザ１によりこのパスワードは変更されてしまう。

【００２４】また、たとえ復旧センター４が悪意を有しており、復旧したパスワードを用いてユーザ１にそれを通知する前にユーザ１が紛失前のパスワードを使用して暗号化しているファイル５を得ようとしても、このファイル５はワークステーション２からのアクセス制御により外から得ることはできないので、内容が知られることはない。

【００２５】次に、請求項２の発明について説明する。請求項１の発明に係る上記実施例では、ユーザ１が暗号化パスワードファイル５をワークステーション２内に保持するものとしていたが、例えばフロッピーディスクなどの可搬な媒体（図示せず）に格納して保管することが考えられる。このことによりユーザ１が自己のパスワードを紛失していない状態でのパスワード復旧センター４から暗号化パスワードへのアクセスがより一層困難になる。このような媒体に格納することによって、ユーザの暗号化パスワードの管理も容易になり、更に安全性が向上する。

【００２６】また、同じく上記実施例においては、ユーザ１は既存の通信手段を用いてパスワード復旧センター４と情報のやり取りを行うものとしているが、これを例えばフロッピディスクのような可搬媒体を郵送する等物理的に搬送する方法で行ってもよい。次に、請求項３の発明を説明する。

【００２７】本発明においては、請求項１の発明に係る上記実施例における（数１）、及び（数２）に示す演算の対象は、ユーザ１のパスワードｕでなく、次に示すようにユーザ１の数値化された識別情報（ＩＤ）と、パスワードを列記した結合パスワードが用いられる。ここに、識別情報とは氏名、住所などパスワード復旧センター４によりユーザ１を特定できる情報である。

【００２８】$C' = (ID \cdot \| u)^e \bmod$（'‖'は結合を示す）…（数３）

パスワード復旧センター４は、この暗号化、パスワードＣ'を復号して得たユーザ１の識別情報を、復旧を要求しているユーザの識別情報と比較する。これにより、ユ

ーザ１の暗号化パスワードを知得した他のユーザが、ユーザ１を詐称してセンターにパスワードの復旧を要求するという不正を排除しえる。

【００２９】次に、請求項４の発明を説明する。本発明においては、請求項１の発明に係る上記実施例における、（数１）及び（数２）に示す演算の対象は、ユーザ１によりパスワードの最終桁に無意味な数字を付加することにより秘密化された秘密パスワードである。この場合、パスワード復旧センター４は、ユーザ１がそのパスワードの最終桁に無意味な数字を付加していることを知らないため、たとえユーザ１のワークステーションに接近しえたとしても、ユーザ１のファイルの内容を知得するのは困難となる。更にまた、ユーザ１が複数の復旧センターを利用してパスワードを２段に暗号化したり、又１のパスワードを分割し、各分割したパスワードを別個独立の複数の復旧センターの公開鍵を使用して暗号化し、復号は各々の復旧センターに依頼し、その上で復号結果を結合することにより紛失したパスワードを復旧するようにしてもよい。このことにより、更に安全性が向上するため、重要な秘密情報や大金を取り扱う場合に極めて有効であろう。

【００３０】次に、請求項５の発明を説明する。本発明においては、請求項１の発明に係る上記実施例における（数１）及び（数２）に示す演算の対象は、ユーザ１が使用する複数のパスワード等である。これにより、単一の公開鍵を使用して複数のパスワードを保管することが可能となる。従って、業務の都合で多数のＬＡＮ、公開通信ネットワークを使用する者等や多数の銀行と取引が有る者等に便利である。

【００３１】しかも、万が一悪意あるパスワード復旧センター４や第三者に暗号化されたパスワードが復号されたとしても、第三者等にとっては復号された個々のパスワードがどのシステムのパスワードか不明であるため、システムの安全性は向上する。ことに、請求項４の発明と組み合わされた場合には、この効果は増大する。次に、請求項６の発明を説明する。

【００３２】上記請求項１の発明に係る暗号化パスワードは、ユーザ１自身若しくはその利用機関においてパスワードとして入力された数値の正否をただちに確かめるために用いることもできる。すなわち、ユーザ１自身若しくはユーザ１の利用機関が、パスワードとして入力した数値をあらかじめ記憶させてある計算プログラムによりパスワード復旧センターの公開鍵をもちいて暗号化した上で表示させ、あらかじめユーザ１により設定の上ユーザ１のものとして登録済の暗号化パスワードと比較して、一致していれば本入力値は第三者でなく、実際にユーザ１により正しく入力されたパスワードであることを確認する。

【００３３】以上、本発明を実施例を中心に説明してきたが、本発明は何も上記実施例等に限定されないのは勿論である。すなわち、上記請求項１の発明の実施例ではパスワード復旧センターによる復旧にＲＳＡ暗号を用いる方式について説明したが、これは公開鍵暗号方式であればどのようなものであってもよいのは勿論である。他の公開鍵暗号方式としては例えばエルガマル暗号がある。このエルガマル暗号については’ア　パブリックキー　クリプトシステム　アンド　シグネチャスキーム　ベイスト　オン　ディスクリート　ロガリズム’（T. E. ElGamal：’A publicK－ey cryptosystem and signature schemebased on discrete logarithm’, Proc. Cr－yptot８４）に詳しく述べられている。なお、上述の「現代暗号理論」には、このエルマガル暗号の他、他の公開鍵暗号方式が幾つか説明されている。さらに、上記実施例及び「現代暗号理論」では整数上の演算が用いられているが、例えば楕円曲線、有限体ＧＦ（Ｐ）上で定義された一次元Ａｂｅｌ多様体（既約で非特異な種数１の射影代数曲線、標数≠２、３の場合には$Y^2 = X^3 + a*X + b$と表される。ここにａ、ｂはＧＦ（Ｐ）の元）を用いた演算であってもよい。

【００３４】また、例えばパスワードは数字でなく「特許庁」、「発明」等の単語であってもよい。また入出力兼用でなく、入力専用、又は出力専用のものであってもよい。識別情報は氏名、住所等でなく郵便番号や企業における従業員番号等の数値であってもよい。識別情報とパスワードの結合も、単に両者を列記するだけでなく、両者を数値情報化した上で掛け算をなす等の秘密処理があわせてなされてもよい。またファイルの具体的意味内容も各種の数値化された情報や銀行預金に限らず、第三者に知られたくない個人的なメモ等も包含するのは勿論である。

【００３５】

【発明の効果】以上、説明したように請求項１の発明においては、パスワード復旧センターはユーザがパスワードを記憶している間はユーザの保持する暗号化パスワードを知り得ず、ユーザのパスワードを求めることはできない。そしてユーザがパスワードの復旧を求めてきたときには、それまで用いていたパスワードを知り得るが、これをユーザに送信した時点でユーザはパスワードを変更してしまうためパスワード復旧センターによる不正は困難である。また、第三者が暗号化パスワードを知り得ても、それを復号できないためユーザのパスワードを知ることは困難である。このため、パスワードを使用した開放的ワークステーションのパスワードの紛失事故にたいする耐性、安全性が向上する。

【００３６】請求項２の発明においては暗号化パスワードは、フロッピディスクのような可搬媒体に格納してそれを設定したユーザ本人が保持するため、よりシステムの安全性が高まる。請求項３の発明においては、ユーザ

9

固有の識別情報が含まれているため、暗号化されたパスワードを取得した第三者の詐称によるパスワードの復旧要請を排除することが可能となり、よりシステムの安全性が高まる。

【００３７】請求項４の発明においては、暗号化され、復号されるパスワード自体に秘密化処理がなされるため、とくに公衆回線等開放的な通信ネットワークを使用し、復旧センターやその利用の信頼性に難がある場合にシステムの安全性が向上する。請求項５の発明においては、複数のパスワードを一体にして保管することが可能となるため、多数のパスワードを利用するユーザの便利性が向上する。

【００３８】請求項６の発明においては、暗号化パスワードを、入力されたパスワードが真にその設定者により正しく入力されたものか否かをただちに調べるために用いることができ、システムの安全性、利用性が高まる。

10

また、第三者の目にふれ易い環境の下でも、パスワード入力者は入力した数値情報をあらかじめ記憶させてある計算プログラムにより暗号化した上で入力装置に表示させることにより、視覚により本当に自分が設定しているパスワードが正しく入力されたか否かを確認の上、次の操作に移る様なことも可能となる。このため、この面からもシステムの安全性、利用性が高まる。

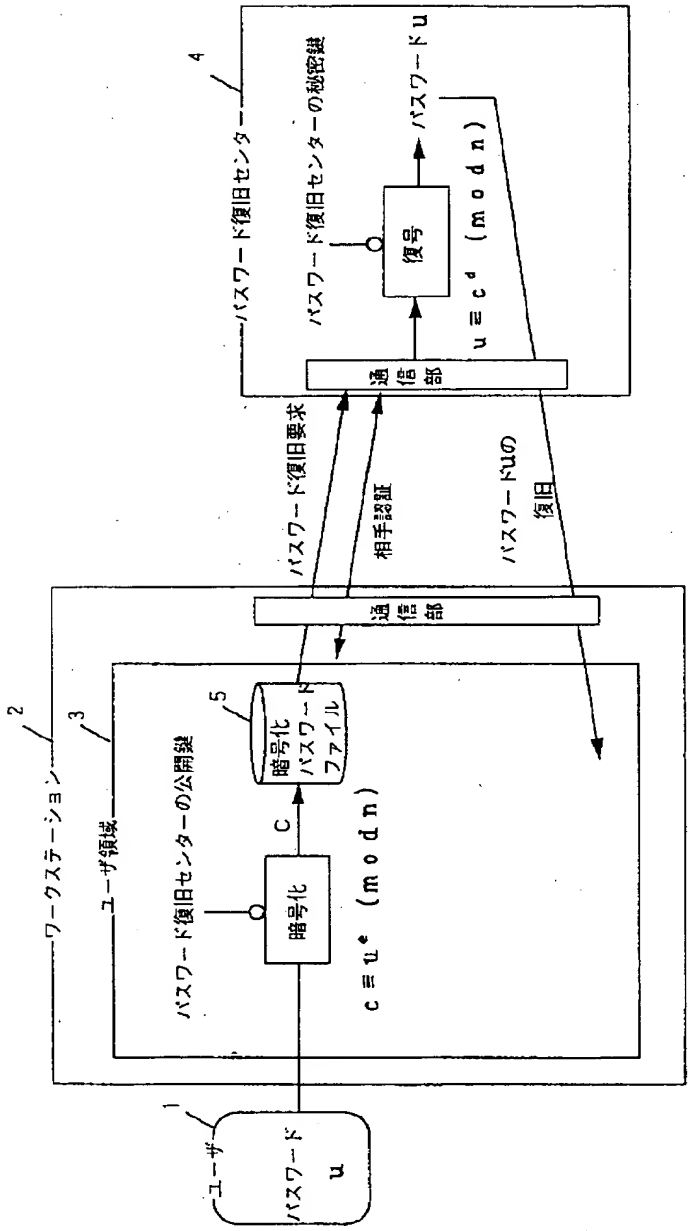
【図面の簡単な説明】

【図１】本発明の一実施例におけるパスワード復旧方式の構成図である。

【符号の説明】

１．ユーザ
２．ユーザの使用するワークステーション
３．ワークステーション内のユーザ１の領域
４．パスワード復旧センター
５．暗号化パスワードファイル

【図１】


パスワード復旧センター
4
パスワード復旧センターの秘密鍵
パスワードu
復号
u ≡ c^d (mod n)
通信部
パスワード復旧要求
相手認証
パスワードuの復旧
通信部
ワークステーション
2
3
ユーザ領域
5
暗号化パスワードファイル
パスワード復旧センターの公開鍵
暗号化
c
c ≡ u^e (mod n)
1
ユーザ
パスワード
u